DEPARTMENT OF STATE
FY 2008
PRIVACY IMPACT ASSESSMENT
Compensation Support

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Programs and Services
Privacy

E-mail: pia@state.gov

FY 2008 Privacy Impact Assessment
for
Information Technology Projects

Introduction

Section 208 of the E-Government Act requires agencies to conduct a privacy impact assessment (PIA) for all new and significantly modified information technology (IT) projects. This includes projects that are require funding from the Office of Management and Budget (OMB), non-major systems requesting funding internally, and those undergoing Department IT Security Certification and Accreditation (C&A) process. The PIA is an analysis of how information is handled to:

- Ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- Determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system;
- Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

The PIA helps DOS employees consider and evaluate whether existing statutory requirements and key information management concepts are being applied to new and modified IT systems that contain personally identifiable information (PII) about members of the public. OMB has oversight of implementation of the Privacy Act of 1974, as amended, for all federal agencies.

It is important to note that OMB closely scrutinizes IT project budget requests on the Exhibit 300 based on the answers given on the PIA. The Exhibit 300 is a part of OMB Circular A-11, *Preparation, Submission and Execution of the Budget*. It is published annually at http://www.whitehouse.gov/omb/circulars/index-budget.html .

In addition to other criteria, major IT projects (requests for over $100,000), especially new initiatives, must score well when OMB evaluates the Exhibit 300 Business Cases. The score obtained on the PIA helps to determine whether funding will be given for the project. IT systems scoring poorly on the PIA will be at risk of not being funded by OMB. The same scrutiny will be applied to non-major funding requests (requests for under $100,000) as well as systems undergoing the C&A process. That being said, it is imperative that the attached PIA be fully **completed, certified, and submitted** via e-mail to pia@state.gov .

The Office of Information Programs and Services in the Bureau of Administration (A/ISS/IPS) is responsible for conducting PIAs on IT systems containing PII as part of its Department-wide implementation of the Privacy Act. IPS reviews and scores all PIAs on Exhibit 300 Business Cases. The score reflects how well your system protects personal information. This score will be integrated with the score for security to obtain an overall score. This combined score is incorporated in the submission of Exhibit 300 to OMB. IPS provides the Exhibit 300 to the Office of Information Assurance for purposes of C&A. For non-major systems, IPS retains PIAs for these systems for future use. A guide and a handbook are being provided along with the PIA questionnaire. If you have addition questions please email us at pia@state.gov.

Department of State
FY 2008 Privacy Impact Assessment

The Privacy Staff (A/ISS/IPS) retains a copy of each completed PIA and copies may be provided to the:

- Bureau/office IT Security Manager, when a C&A is required; and
- Office of Management and Budget (OMB) Capital Planning Exhibit 300 Submission when an Exhibit 300 is required.

Please note that you will receive a low score if all appropriate questions are not adequately answered and/or if the certification page is not completed fully. A guide and handbook are provided along with the PIA questionnaire. **You must refer to the handbook as you complete the PIA. The handbook mirrors each section of the PIA and provides instructions for each question.** For more detailed information, please refer to the guide.

A. CONTACT INFORMATION

(5) Who is the Agency Privacy Coordinator who is conducting this assessment? (Name, organization, and contact information).

Ms. Charlene Thomas
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy (PRV)

B. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION

(1) Does this system collect, maintain or disseminate personally identifiable information (PII) about individual members of the public?**

**** "Personally identifiable information from/about individual members of the public" means personally identifiable information from/about "any person not acting in his/her official capacity as a federal government employee/contractor".**

YES X NO___

If the above answer is YES, please complete the survey in its entirety. If NO, complete the certification page and submit the PIA to the following e-mail address: pia@state.gov.

1) Does a Privacy Act system of records already exist?

YES X NO___

If yes, please provide the following:
System Name: Personnel Payroll Records, Number STATE-30

If no, a Privacy system of records description will need to be created for this data.

2) What is the purpose of the system/application?

To manage payroll and retirement compensation. Compensation Support includes the Consolidated American Personnel Payroll System (CAPPS), the Foreign Affairs Retirement and Disability System (FARADS), the Annuity Benefit and Retirement Calculator (ABC), the Retirement Record System (RRS), and the reporting tool, Report.Web.

3) What legal authority authorizes the purchase or development of this system/application?

31 U. S. Code 901-902

C. DATA IN THE SYSTEM:

1) What categories of individuals are covered in the system?

Department of State employees and their family members.

2) What are the sources of the information in the system?

a. Who/what is the source of the information?

Department of State employees.

b. What type of information is collected from the source of the information?

- **Reporting and Information;**
- **Budget and Finance;**
- **Monitoring;**
- **Payments;**
- **Collections and Receivables;**
- **Central Fiscal Operations;**
- **Income Information;**
- **General Retirement and Disability;**
- **Survivor Compensation;**

- **Budget Execution; and**
- **Debt Collection**

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

All data is collected electronically, using industry-standard file transfer utilities or *via* electronically encrypted email. Once received, data is validated by compensation analysts prior to use.

b. How will data be checked for completeness?

Employees provide updates, as needed, and can correct errors or omissions.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).
The employee can view the data on the earnings and leave statement and can update his or her record.

D. <u>INTENDED USE OF THE DATA:</u>

1) Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?

Yes

2) Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?

No data derivation nor aggregation is involved in the application.

3) Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?

Members of the public do not have access to this system.

4) Will the new data be placed in the individual's record?

Yes.

5) How will the new data be verified for relevance and accuracy?

Time and attendance data will be verified by the employee's timekeeper; the employee can also request the data be updated, as needed.

6) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

Data is retrieved by job control language as the payroll analyst requires. Personal identifiers include employee name, employee number and social security number.

7) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

The reports are used to manage the functions of the system, including payroll, retirement compensation, benefit accrual, etc. Employees in the Charleston Financial Service Center and the Operations and Maintenance team have access to these reports. There are over 1,000 reports (and we can provide the titles), but few of them relate to non-employees. Those that do:

CAPPS

REPORT TITLE
AGENCIES PAID BY STATE
SEPARATED EMPLOYEE GARNISHMENTS
SEPARATED EMPLOYEES RETIREMENT
PEACE CORPS 113-A REPORT
EMPLOYEES SEPARATIONS REPORT

FARADS

REPORT TITLE
CHILD ANNUITS AND SURVIVORS
DECEASED ANNUITANTS, SURVIVORS
FORMER SPOUSES WITH HEALTH BENEFITS NO HB STATUS
FORMER SPOUSES WITH HEALTH BENEFITS (CURRENT, ADJ)
RECENTLY RETIRED/DECEASED ANNUITANTS
SURVIVORS & FORMER SPOUSES
SURVIVOR SPOUSE LIST

E. MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

The Compensation Support System is operated in only one site.

2) **What are the retention periods of data in this system?**

Retention of these records varies from 3 to 99 years, depending upon the specific kind of record involved. They are retired or destroyed in accordance with published records schedules of the Department of State and as approved by the National Archives and Records Administration (NARA).

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

This function is performed programmatically; the job control language contains the definitions and procedures

4) **Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No.

5) **How does the use of this technology affect public/employee privacy and does it restrict access to the system?**

N/A

6) **If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?**

Transaction logs record user activity; Information System Security Officers and payroll analysts can access these logs.

7) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

If the system is modified, Privacy Act system of records notices would be revised as necessary.

8) **Are there forms associated with the system? YES X NO ___**
If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?

The Access Control Facility (ACF) 2 log-on request form [This form is used solely to document the user receiving credentials for the system, and lists only Department employees and contractors, not family members or members of the general public].

F. **ACCESS TO DATA:**

1) **Who will have access to the data in the system?** (e.g., contractors, users, managers, system administrators, developers, other)

Operations and maintenance personnel, employees of the Charleston Financial Service Center (payroll technicians who can edit records as needed); users can review their own records and request updates as necessary.

2) **What are the criteria for gaining access to the system?** Are criteria, procedures, controls, and responsibilities regarding access documented?

The Table-driven On-line Foundation Software was developed by American Management Systems, Inc. at the request of the Department. This software provides transaction control, reference tables and the application interface. This software runs on the IBM Transaction Server (also known as the Customer Information Control System, CICS) and is joined to the Computer Associates' Access Control Facility (ACF) 2 security control. The combination of TOFS and ACF2 provides extremely tight security for this sensitive but unclassified mainframe-based system. These procedures are documented in operations and maintenance manuals.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

   Payroll technicians can see all data; operations and maintenance personnel typically run jobs and can view individual records, but not with update access.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access?** (Please list processes and training materials)

   ACF2 user profile record specifies which applications or classes of applications the user is entitled to execute. The user is only permitted to use the application(s) within the security class assigned in the profile. The fields in this user profile record include:

   - **Userid. This must match the ACF2 logon id used to sign on to CICS and is used as the retrieval key.**
   - **User's name. Used for statistical reports and administrative purposes.**
   - **User's SSN. Used to disallow access to data records pertaining to the individual user.**
   - **User's Organization Code. Used to restrict access to data records (used to separate BBG access).**
   - **Printer terminal ID. Controls the printer to which the user is authorized to route transaction prints.**
   - **User's primary menu screen. Determines the initial TOFS menu that will be displayed when the user signs on. (This is a convenience feature rather than an essential security control and can be overridden by the user.)**
   - **Application classes. A list of the classes (groups of transactions) the user is authorized to execute.**
   - **Application transactions. An optional list of individual transactions for which the user is authorized in addition to the classes of transactions. (This extends the potential granularity of control to the level of individual transactions.)**

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system**? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?

   Contractors and government staff work together in support of Compensation Systems. Privacy Act contract clauses and rules of conduct are in place.

6) **Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

   Data from this system goes to other agencies including Department of Health and Human Services, Social Security Administration, Department of the Treasury, Office of Personnel Management, and the Federal Reserve Bank. These interfaces are encrypted.

7) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? If so, how will the data be used by the other agency?**

   No.

8) **Who is responsible for assuring proper use of the SHARED data?**

   The Operations and Maintenance Team assures secure transport of the shared data.

ADDITIONAL COMMENTS: *(optional)*